Meru Connect

15.10
Release Notes

Meru Connect (**MCT**) is a complete provisioning, management, and reporting system that provides temporary network access for guests, visitors, contractors, consultants, or customers. Meru Connect works alongside Wireless Controllers, LAN Switches, NAC Systems, Firewalls and other Network Enforcement devices which provide the captive portal and enforcement point for guest access.

This release comes with important fixes and the following new features. See the Meru Connect 15.10 user guide for details about the following features

- Support for TACACS+ Authentication Server
  - Admin users can now use TACACS+ authentication server
- Enhancements to Reporting
  - Two new reports are available for sponsor users. You can now create AP usage summary and user activity report.
- Captive Portal integration with FortiGate.
- Smartconnect now supports Windows 10, iOS 9, OS X 10.11 (El Capitan)
- Prevent re-use of Self-Service account
  - Prevents the creation of self-service accounts with the same personal details (email/phone) for a specified period of time post the original account creation.
- Support for WiForia (3rd party Wi-Fi based marketing notification services)
- Add accounts to an existing batch
  - New accounts can be added to an existing batch by specifying its name at account creation time.
- New API to enable or disable Remember Me option
  - This API can disable the *Remember Me* option of a guest till they enabled it again.
- Ability to delete event code after expiry
  - A sponsor can now delete an expired event code from the Manage event codes page
- OAuth support is enhanced to collect additional user details
- Support to push custom captive portal profile settings to SD 8.0 controller
  - Custom captive portal profile is a new feature in SD 8.0 that allows you to create individual captive portal profiles with distinct configuration settings. You can specify a custom captive profile in Meru Connect and push that configuration to SD 8.0 controller.

Fixed Issues

BugID	Description
44237	Fixed issued that caused problems while joining an AD domain.
48309	Device Account creation fails with SQL error visible in the logs
48347	Smart Connect on Android Unable to connect when multiple root certs are selected
49534	"Remember me" fails on certain condition against the external radius server
49463	iOS/OSX profile contains empty credentials plist elements
49937	Authorization profile AV pair is clearing out on adding a device restriction
49991	Fixed missing MIB files (used for CP integration with HP switch) on some MCT installations
49337	Fixed issues related to captive portal theme's responsive rendering on screen reader
48387	Under certain conditions authentication fails for AD user who belongs to multiple groups
49573	Fixed sponsor approval email link issues with MCT running on Meru Centre

Known Issues

- Mac/iPad in a FortiGate set up will intermittently timeout guest authentication and delay success page redirection. This is noticed when authentication is done using Safari browser.
- When integrating with Fortigate, Oauth authentication is not supported.
- When running SC on Ubuntu, if the user provides incorrect credentials the system might prompt the user to select a certificate for authentication.
- Smart Connect Ubuntu app can becomes unresponsive when configuring PSK profile.

Upgrade Path

Supported Hardware and Software

Hardware

The following hardware products are supported for this release:

Supported	SA250, SA2000

Virtual Machine

- ESX 3.5
- ESX 3.5i
- ESX 4.x
- ESX 4.xi
- ESX 5.xi
- ESX 6.0
- Microsoft Hyper V on Windows 2008 or later
- Workstation 5.0 or later
- Fusion 2.0 or later

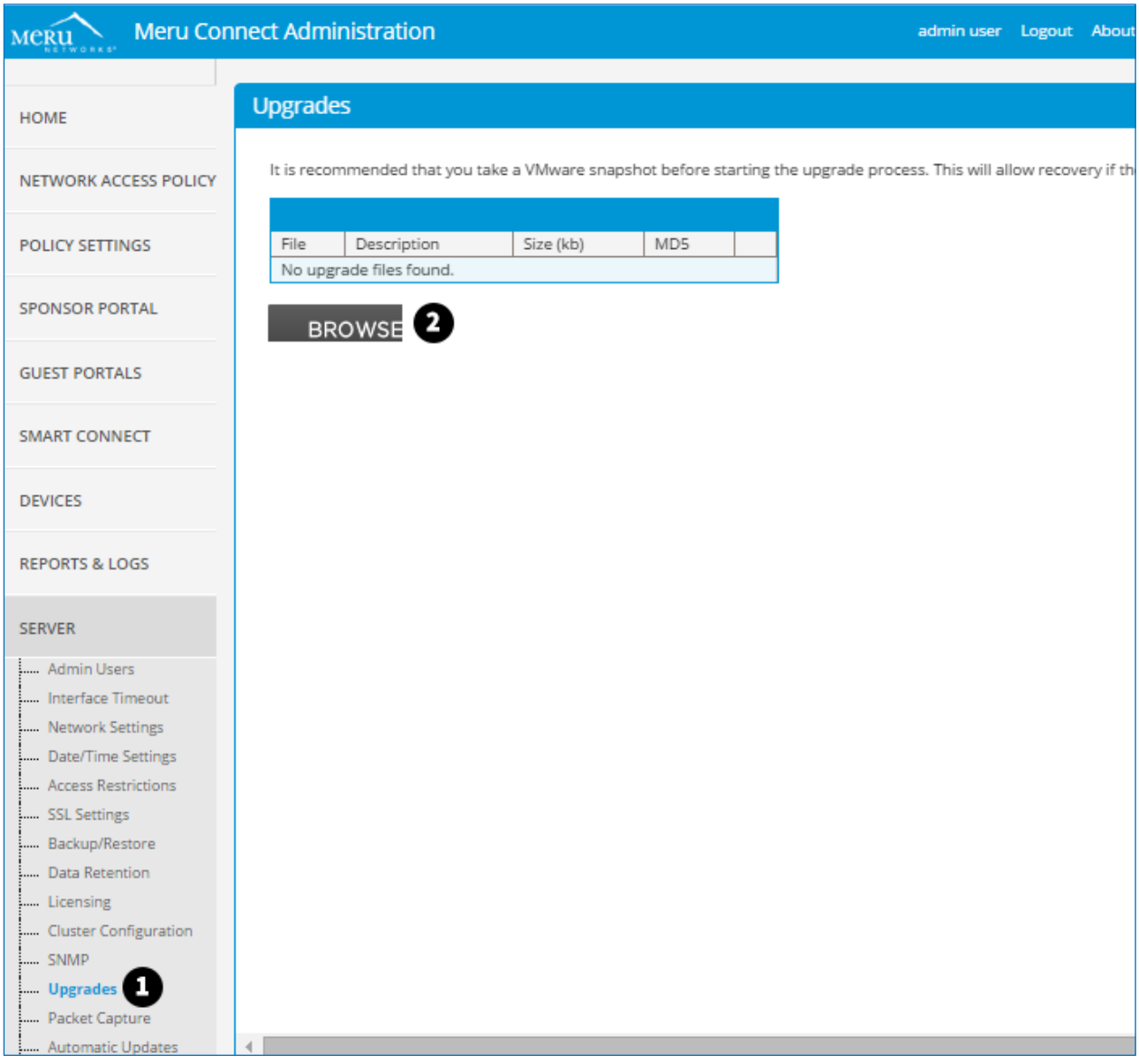
NOTE	Workstation and Fusion versions are only supported for evaluation or demonstration purposes.

Upgrade Process

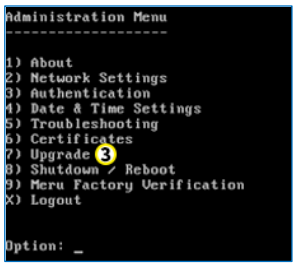
From the CLI Administration menu you can perform an upgrade of your Meru Connect. To allow this you must have already uploaded the upgrade file to your Meru Connect; this can be done via the Meru Connect administration interface once you have logged on for the first time.

NOTE	All previous releases of Identity Manager or Guest Manager must be upgraded to 14.2 before upgrading to Meru Connect 15.10. If running from SSH do not close the session or lose network connectivity as this will terminate the upgrade and cause potential issues. To avoid this problem you can run the upgrade from the appliance console.

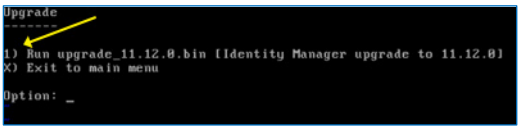
1. From the Meru Connect Admin select Server and click on Upgrades (**1**) as shown below.



2. Click on the browse button (**2**) and select the upgrade file from your locally stored directory. The file should upload automatically.
3. From the CLI Administration Menu select option 7.



4. Select option 1 to perform the upgrade.



Licensing and Initial Configuration

Meru Connect requires a license file before it can run. For instructions on initial system setup and how to obtain a license, refer to Chapter 4 (System Setup) of the Meru Connect User Guide.

Additional Resources

In addition to the release notes, the following documentation is available.

- Meru Connect User Guide
- System Director 8.0 Configuration Guide

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Support and Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service